



BeyondTrust

Privileged Remote Access 22.2 Privileged Web Access Console

Table of Contents

Privileged Web Access Console Guide	4
Privileged Web Access Console Requirements	5
Platforms	5
Browsers	5
Launch the Web Access Console	6
Launch the Web Access Console Using /console	6
Launch the Web Access Console Using /login	6
Launch the Privileged Web Access Console from the User Drop Down Menu	7
Use Jump Items to Access Endpoints in the Privileged Web Access Console	8
End-User and Third-Party Authorization	9
Revoke an Access Approval Request	10
Automatic Log On Credentials	12
Log Into Endpoints Using Credential Injection	13
Install and Configure the Endpoint Credential Manager	13
System Requirements	13
Install and Configure the Plugin	15
Configure a Connection to Your Credential Store	16
Use Credential Injection to Access Endpoints	17
Check In and Check Out Credentials	18
Authenticating from the Client Scripting API	19
Return to an Active Session in the Privileged Web Access Console	20
Search for Endpoints	20
Control the Remote Endpoint with Screen Sharing Using Privileged Web	21
Screen Sharing Tools	21
Open the Command Shell on the Remote Endpoint Using the Privileged Web Console	23
Command Shell Tools	23
View System Information on the Remote Endpoint	24
System Information Tools	24
Use the Privileged Web Console to Transfer Files to and from Remote Systems	25
File Transfer Tools	26

Share a Session with Team Members or External Users Using the Privileged Web Access Console	27
Invite Team Members	27
Invite External Users	28
Remove a Member from a Privileged Web Access Console Session	31
Close the Privileged Web Access Console Session	32
Download the Native Desktop from the Privileged Web Access Console	33

Privileged Web Access Console Guide

With the BeyondTrust privileged web access console, Information and Cyber Security teams can grant privileged users secure remote access to critical systems, even when those users do not have the ability to install software within their own desktop environments. Instead, they can access endpoints through the web-based access console. This ensures that the necessary access can always be granted and enables system owners to meet business requirements, such as system up-time and any other internal or external regulations without compromising defenses put in place to protect their organization from any sort of malicious cyber threat.

In this guide, we will specifically discuss the privileged web access console and how this browser-based access console accesses endpoints and performs other necessary functions while ensuring that the highest level of security is maintained.



Note: Use this guide only after an administrator has performed the initial setup and configuration of the B Series Appliance as detailed in the [BeyondTrust Appliance B Series Hardware Installation Guide](#). Should you need any assistance, please contact BeyondTrust Technical Support at www.beyondtrust.com/support.

Privileged Web Access Console Requirements

To run the privileged web access console on your system, your B Series Appliance must be running software version 15.3 or higher. The privileged web access console is supported on the following platforms and browsers:

Platforms

- Windows
- Macintosh
- Linux

Browsers

- Chrome 46+
- Firefox 42+
- Internet Explorer 11+
- Safari 8+
- Windows Edge



IMPORTANT!

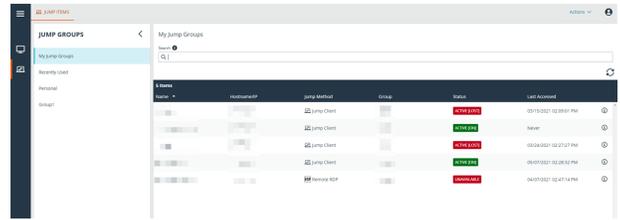
Your B Series Appliance must be equipped with a valid SSL certificate signed by a certificate authority. Once you have applied a CA-signed SSL certificate to your B Series Appliance, contact BeyondTrust Technical Support. Your support representative will create a new software build that integrates your SSL certificate. With this updated build installed on your B Series Appliance, you can run the BeyondTrust access console on your device to access your endpoints from virtually anywhere.

Launch the Web Access Console

The privileged web access console enables you to securely access your endpoints by connecting to them remotely through the B Series Appliance. To begin accessing endpoints using the privileged web access console, follow the steps outlined below.

Launch the Web Access Console Using /console

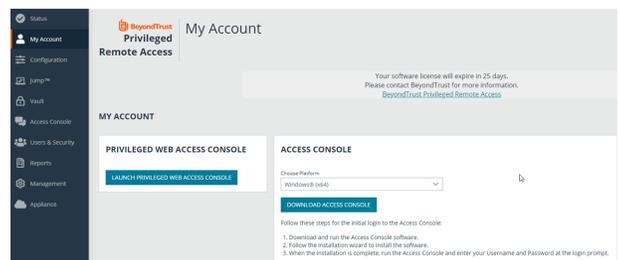
1. In the address bar of your browser, enter your BeyondTrust site hostname followed by **/console**, for example, **access.example.com/console**.
2. Enter the username and password associated with your BeyondTrust user account.
3. Click **Login** to start your web-based access console session.



Launch the Web Access Console Using /login

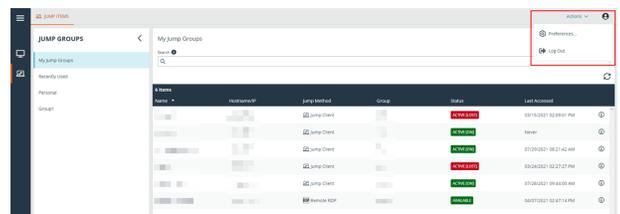
 **Note:** By default, the **Launch Privileged Web Access Console** button is not available in the **/login** administrative interface. You must navigate to **Management > Security** and check **Allow Mobile Access Console and Privileged Web Access Console to Connect** to activate the console.

1. In the address bar of your browser, enter your BeyondTrust site hostname followed by **/login**, for example, **access.example.com/login**.
2. Enter the username and password associated with your BeyondTrust user account.
3. Click **Login**.
4. Select **My Account**.
5. Click **Launch Privileged Web Access Console**.



6. The privileged web access console opens in a new tab, and you can begin accessing endpoints.

To log out of the access console, click **Logout** in the upper right corner of the screen.

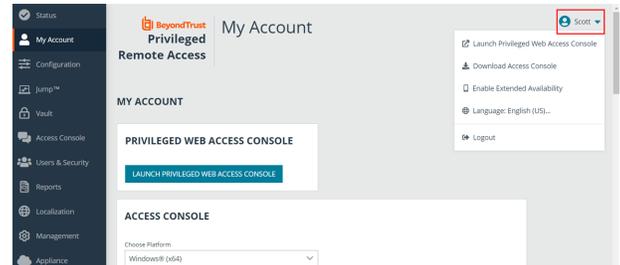


Launch the Privileged Web Access Console from the User Drop Down Menu

You can also launch the Privileged Web Access Console from the User dropdown menu located on the right upper corner of the UI. This menu is accessible from any tab location in the administrative site.



Note: If you have more than one language enabled on your site, you can change the language used in the Privileged Web Access Console by clicking on the **Languages** link in the User dropdown menu and selecting the language you want. This language is applied to both the /login site and the Privileged Web Access Console.



Use Jump Items to Access Endpoints in the Privileged Web Access Console

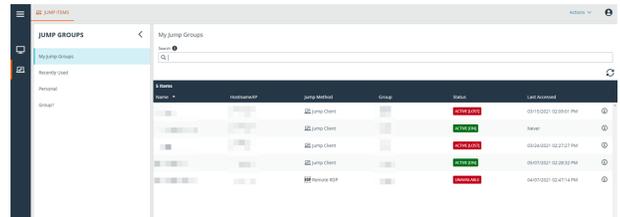
To access an endpoint, install a Jump Item on that system from the **Jump Clients** page of the /login administrative interface.

Jump Items are listed in Jump Groups. If you are assigned to one or more Jump Groups, you can access the Jump Items in those groups, with the permissions assigned by your admin.

Your personal list of Jump Items is primarily for your individual use, although your team leads, team managers, and users with permission to see all Jump Items may have access to your personal list of Jump Items. Similarly, if you are a team manager or lead with appropriate permissions, you may see team members' personal lists of Jump Items. Additionally, you may have permission to access Jump Items in Jump Groups you do not belong to and personal Jump Items for non-team members.

There are three ways that you can begin accessing endpoints:

- Locate and select an endpoint from the **My Jump Groups** list.
- Choose a Jump Group and then select an endpoint from that group's listing of endpoints.
- Select a session from the **Frequently Used Jump Items** list.

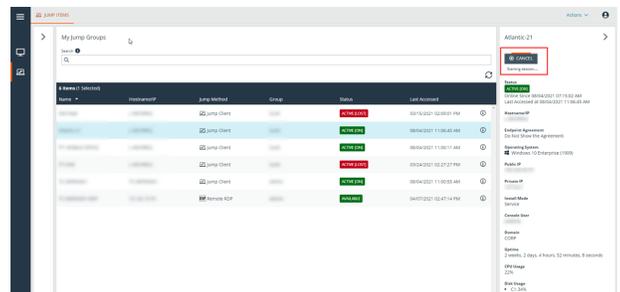
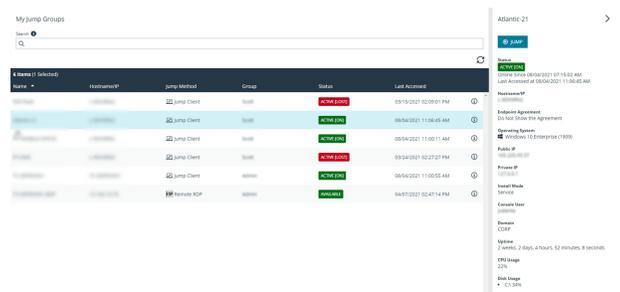


Note: The **Frequently Used Jump Items** list displays all of the Jump Items that you access on a regular basis. To start a session with a frequented item, hover your mouse over the session and click **Start Session**.

Note: The **Jump Items** list can only display a maximum of 50 Jump Items.

To begin accessing Jump Items, follow the steps outlined below:

1. Select a Jump Group and click the **Refresh** button.
2. A list of all Jump Items populates, and you can review details about the Jump Item, including: **Name**, **Method**, **Group**, **Status**, and **Last Accessed**. To review more details about the Jump Item, click on the plus sign beside the Jump Item's name.
3. Click the **JUMP** button to start a session with the endpoint.
4. To cancel a Jump access request, click **Cancel**.



End-User and Third-Party Authorization

Depending on the configuration of Jump Items within the /login administrative interface, a Jump Item may have a Jump Policy associated with it, and the policy may define an authorization component that forces you to request permission from a third-party or an administrator before you are able to start an access session with the Jump Item.

i For more information about how to configure third party and end-user notifications and approval, please see [Jump Policies: Set Schedules, Notifications, and Approval for Jump Items](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-policies.htm) at <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-policies.htm>.

1. After you have clicked the **JUMP** button and requested access, a prompt appears, and you are required to enter a reason for wanting to access the system.

You must first request approval to access this Jump Item. Please confirm the details below and describe the reason for the access request.

Jump Policy:

Jump Policy Description:

Approver(s):

Access Approval Applies To:
Yourself Only

Language:
en-us

Request Reason:

CANCEL OK

2. Next, you must indicate when and for how long you will be accessing the system.
3. Once the request has been submitted, the third party or person responsible for approving access requests is alerted through an email notification and has the opportunity to accept or deny the request. Although other approvers can see the email address of the person who approved or denied the request, the requester cannot.

Please enter the duration for this authorization request.

Start date and time:

07/28/2021 09:13

Duration

2 hours

CANCEL SEND

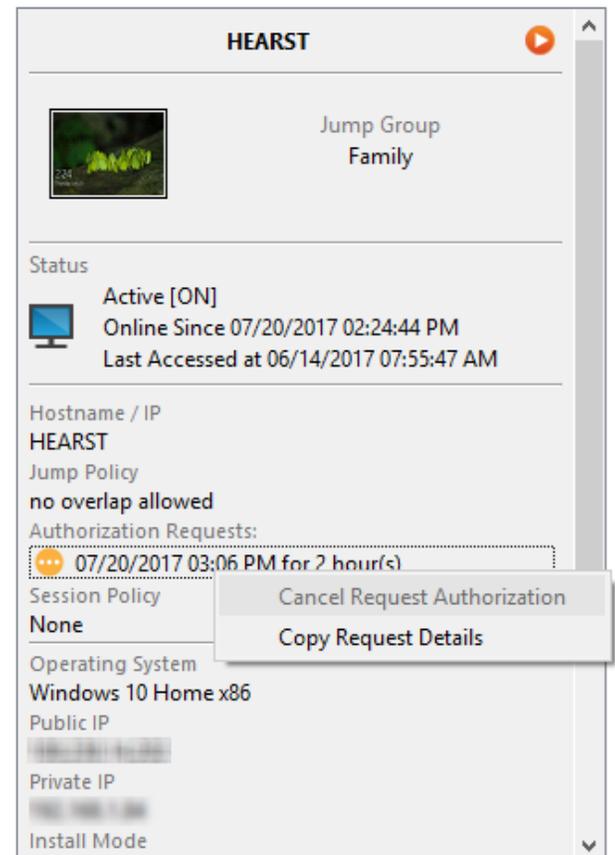
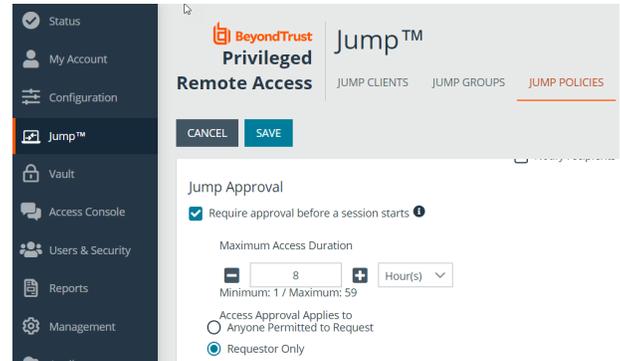
4. After permission has been determined, an authorization notification appears within the Jump Item's information displaying either *approved* or *denied*. If access is granted, you can tap the Jump button to begin accessing the system.
5. Then you are presented with a message asking if you would like to begin an access session.
6. If you choose to begin the session, the approving party's comments appear, and you can begin accessing the system.

Revoke an Access Approval Request

Permission to revoke approved access requests is controlled by Jump Policy. In the **/login** web management interface, go to **Jump > Jump Policies**. Under **Jump Approval** you have two options:

- **Anyone Permitted to Request**
- **Requester Only**

If the Jump Policy is set to **Requester Only**, and an Access Request is presently approved for User A, User B is asked to create a new Access Request if they attempt to Jump to the Jump Item, since that request does not apply to them. Additionally, if User B attempts to cancel the Access Approval Request, the option is grayed out. The only user who can cancel the approved request is User A, because they are the approved user for the request.



However, if the Jump Policy is set to **Anyone Permitted to Request**, and an Access Request is presently approved for User A, User B is allowed to start a new session with the Jump Item if they attempt to Jump to it. In addition, anyone with permission to access the Jump Item is allowed to cancel / revoke the request.

HEARST
▶



Jump Group
Family

Status

 **Active [ON]**
 Online Since 07/20/2017 02:24:44 PM
 Last Accessed at 06/14/2017 07:55:47 AM

Hostname / IP
HEARST

Jump Policy
overlapping authorization allowed

Authorization Requests:

⋯ 07/20/2017 02:2

Session Policy
None

Cancel Request Authorization
 Copy Request Details

Operating System
Windows 10 Home x86

Public IP
[REDACTED]

Private IP
[REDACTED]

Install Mode
Service

Automatic Log On Credentials

Credentials from the **Endpoint Credential Manager** can be used for RDP and for performing Remote Jump. If a user selects to Jump to a Remote Jump or Remote RDP and no automatic log on credentials are available, a username and password must be entered into the prompt before the access session can begin with the endpoint. If the /login administrative interface has been configured with automatic log on credentials and returns only one set of credentials as being available for a particular user and Jump Item, the credential request is skipped, and the single credential is used to start the session. If there is more than one credential configured in the /login administrative interface, the user has the choice either to choose credentials from the credential store or to enter their own credentials manually.

i For more information on credential configuration and management, please see [Security: Manage Security Settings](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/security.htm) at www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/security.htm.

These credentials will be used to connect to [REDACTED].

Credential Store
 Specific User

Search Credentials

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

CANCEL

Log Into Endpoints Using Credential Injection

When accessing a Windows-based Jump Item via the privileged web access console, you can use credentials from a credential store to log into the endpoint or to run applications as an admin.

Before using credential injection, make sure that you have a credential store or password vault available to connect to BeyondTrust Privileged Remote Access.

Install and Configure the Endpoint Credential Manager

Before you can begin accessing Jump Items using credential injection, you must download, install, and configure the BeyondTrust Endpoint Credential Manager (ECM). The BeyondTrust ECM allows you to quickly configure your connection to a credential store, such as a password vault.

 **Note:** The ECM must be installed on your system to enable the BeyondTrust ECM Service and to use credential injection in BeyondTrust Privileged Remote Access.

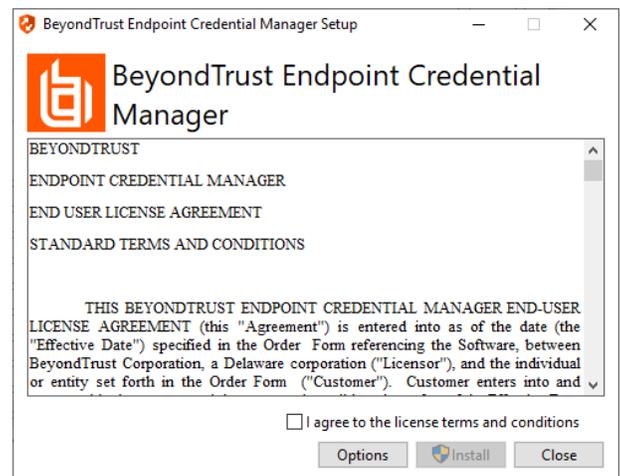
System Requirements

- Windows Vista or newer, 64-bit only
- .NET 4.5 or newer
- Processor: 2GHz or faster
- Memory: 2GB or greater
- Available Disk Space: 80GB or greater

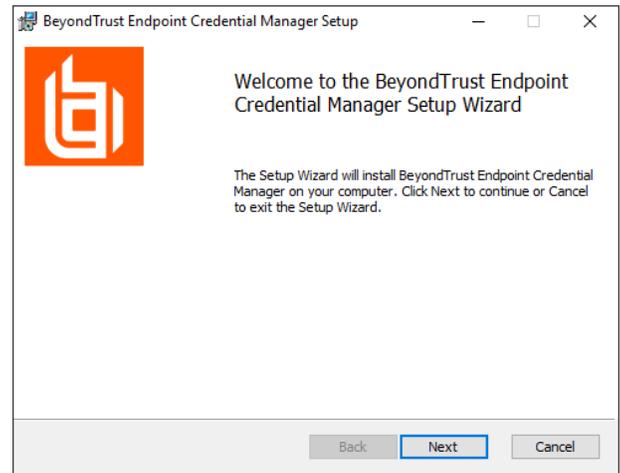
1. To begin, download the BeyondTrust Endpoint Credential Manager (ECM) from [BeyondTrust Support](#) at beyondtrustcorp.service-now.com/csm.
2. Start the BeyondTrust Endpoint Credential Manager Setup Wizard.
3. Agree to the EULA terms and conditions. Check the box if you agree, and then click **Install**.

If you need to modify the ECM installation path, click the **Options** button to customize the installation location.

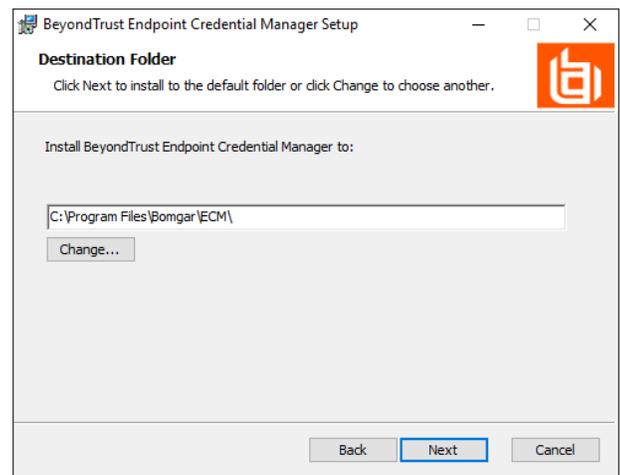
 **Note:** You are not allowed to proceed with the installation unless you agree to the EULA.



4. Click **Next** on the Welcome screen.

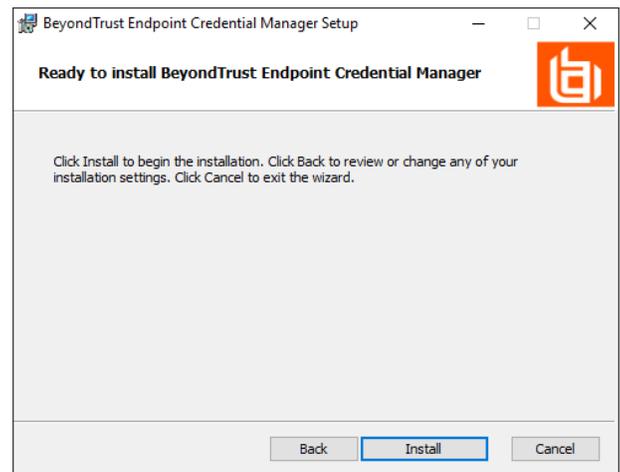


5. Choose a location for the credential manager, and then click **Next**.

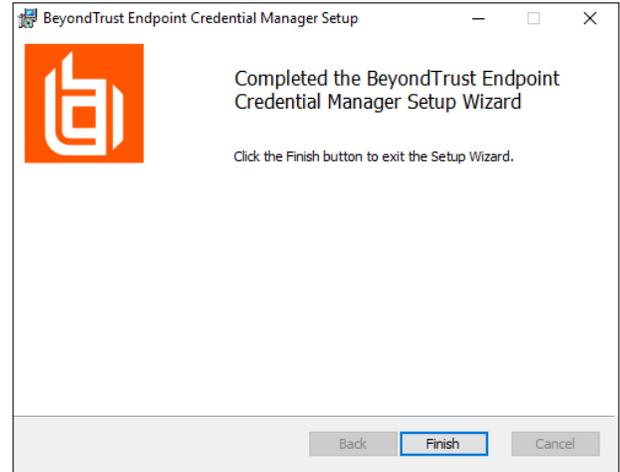


6. On the next screen, you can begin the installation or review any previous step.

7. Click **Install** when you are ready to begin.



- The installation takes a few moments. On the **Completed** screen, click **Finish**.

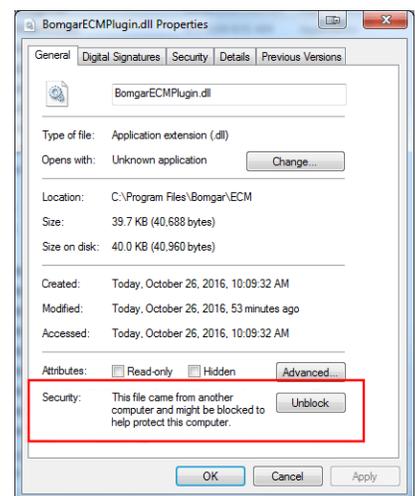


Note: To ensure optimal up-time, administrators can install up to three ECMs on different Windows machines to communicate with the same credential store. A list of the ECMs connected to the appliance site can be found at **/login > Status > Information > ECM Clients**.

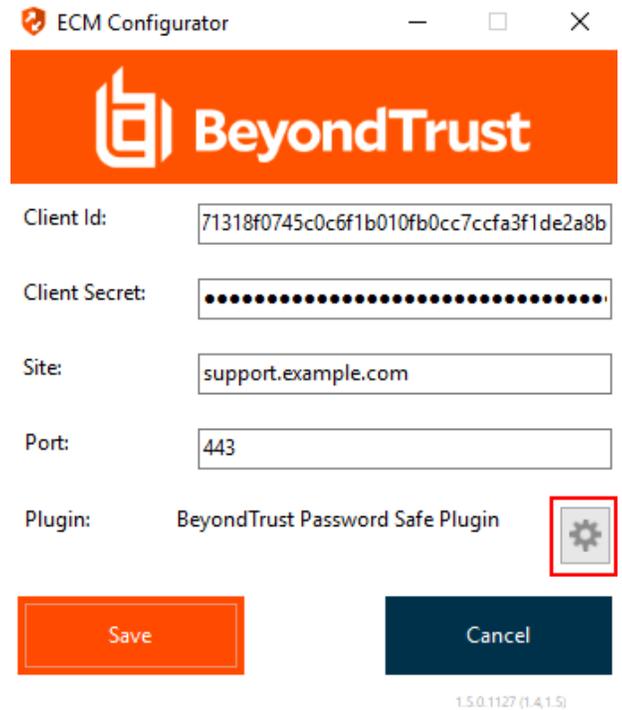
Note: When ECMs are connected in a high availability configuration, the BeyondTrust Appliance B Series routes requests to the ECM in the ECM Group that has been connected to the appliance the longest.

Install and Configure the Plugin

- Once the BeyondTrust ECM is installed, extract and copy the plugin files to the installation directory (typically **C:\Program Files\Bomgar\ECM**).
- Run the **ECM Configurator** to install the plugin.
- The Configurator should automatically detect the plugin and load it. If so, skip to step 4 below. Otherwise, follow these steps:
 - First, ensure that the DLL is not blocked. Right-click on the DLL and select **Properties**.
 - On the **General** tab, look at the bottom of the pane. If there is a **Security** section with an **Unblock** button, click the button.
 - Repeat these steps for any other DLLs packaged with the plugin.
 - In the Configurator, click the **Choose Plugin** button and browse to the location of the plugin DLL.



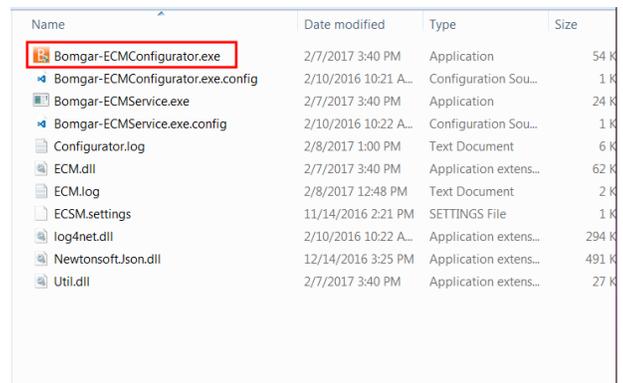
- Click the gear icon in the **Configurator** window to configure plugin settings.



Configure a Connection to Your Credential Store

Using the ECM Configurator, set up a connection to your credential store.

- Locate the BeyondTrust ECM Configurator you just installed using the Windows Search entry field or by viewing your **Start** menu programs list.
- Run the program to begin establishing a connection.



- When the ECM Configurator opens, complete the fields. All fields are required.

Enter the following values:

Field Label	Value
Client ID	The ID for your credential store.
Client Secret	The secret key for your credential store.
Site	The URL for your credential store instance.

Field Label	Value
Port	The server port through which the ECM connects to your site.
Plugin	Click the Choose Plugin... button to locate the plugin.

- When you click the **Choose Plugin...** button, the ECM location folder opens.
- Paste your plugin files into the folder.
- Open the plugin file to begin loading.

Name	Date modified	Type	Size
ECM.dll	2/7/2017 3:40 PM	Application extens...	62 KB
log4net.dll	2/10/2016 10:22 A...	Application extens...	294 KB
Newtonsoft.Json.dll	12/14/2016 3:25 PM	Application extens...	491 KB
Util.dll	2/7/2017 3:40 PM	Application extens...	27 KB



Note: If you are connecting to a password vault, more configuration at the plugin level may be needed. Plugin requirements vary based on the credential store that is being connected.



IMPORTANT!

To apply new settings in the configuration, restart the ECM service.

Use Credential Injection to Access Endpoints

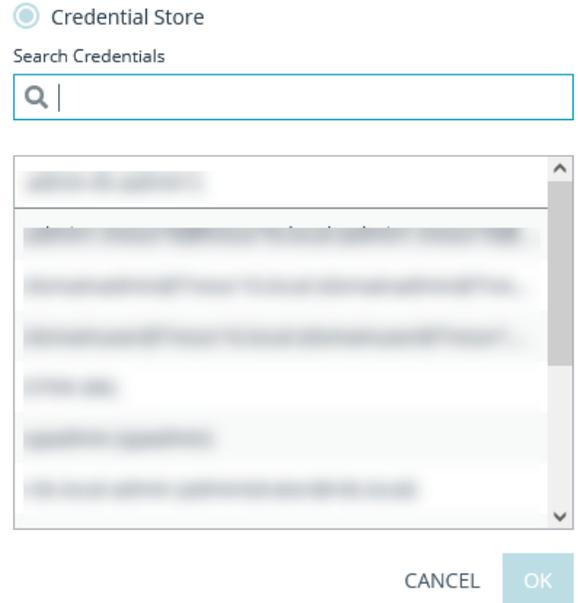
After the credential store has been configured and a connection established, the privileged web access console can begin using credentials in the credential store to log into endpoints.

- Log into the privileged web access console.
- Jump to an endpoint with a Jump Item installed as an elevated service on a Windows machine.
- Click the **Play** button to begin screen sharing with the endpoint. If the endpoint is at the Windows login screen, the **Inject Credentials** button is highlighted.
- Click the **Inject Credentials** button. A pop-up credential selection dialog appears, listing the credentials available from the ECM.



5. Select the appropriate credentials to use from the ECM. The system retrieves the credentials from the ECM and injects them into the Windows login screen.
6. The user is logged in to the endpoint.

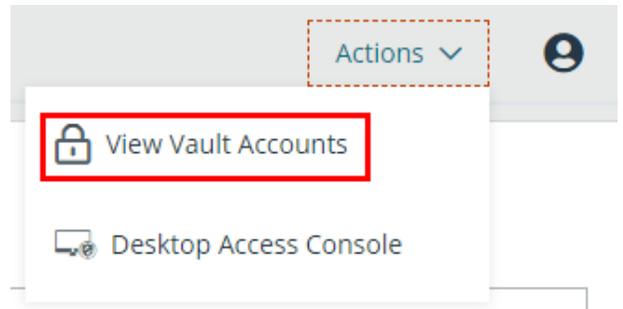
Please select a credential to perform this action.



Check In and Check Out Credentials

From the web access console, you can easily access the Privileged Remote Access Vault in the /login interface to check out and check in credentials when necessary, either during a session or on your local machine.

To access the vault, click the **Actions** dropdown in the top navigation bar and select **View Vault Accounts**. You are taken directly to the **Vault > Accounts** page in the /login interface, once logged in.



You can then locate and check out or check in a Vault account.



Authenticating from the Client Scripting API

This feature allows users to log in to the privileged web access console and Jump to an endpoint using the [PRA Client Scripting API](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/client-script/index.htm#client-scripting-api) (<https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/client-script/index.htm#client-scripting-api>).

The Client Scripting API URL follows the format of `https://access.example.com/api/client_script`, where `access.example.com` is your B Series Appliance hostname.

The API accepts a client type (`web_console`), an operation to perform (`execute`), and a command (`start_jump_item_session`). No other commands are supported for the `web_console` client type.

If the user is logged into the desktop access console when the Client Scripting API URL is accessed with `type=web_console`, then the user is logged into the privileged web access console and disconnected from the desktop access console. If this behavior is not desired, then the user must use a Client Scripting API URL with `type=rep` instead of `type=web_console`.

Conversely, if the user is logged into the privileged web access console and the API calls `type=rep`, the user is logged into the desktop access console and disconnected from the privileged web access console.

Here is an example of a valid Client Scripting API request:

```
https://access.example.com/api/client_script?type=web_console&operation=execute&action=start_jump_item_session&search_string=ABCDEF02
```

If the user is already logged into the privileged web access console, the above request runs the command in the browser tab running the privileged web access console. In this case, the command starts a session with the Jump Client whose hostname, comments, public IP, or private IP matches the search string "ABCDEF02."

If the user is not already logged into the privileged web access console, the above request opens a new browser tab and directs the user to `/login` to authenticate (this step is skipped if the user is already logged in to `/login`). The user is then redirected to the privileged web access console, and the command starts a session with the Jump Client whose hostname, comments, public IP, or private IP matches the search string "ABCDEF02."

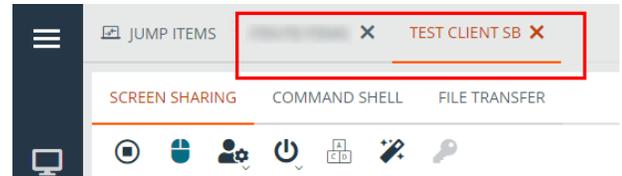
In both cases, if more than one Jump Item matches the search criteria, the user must select the correct Jump Item from a list. If no Jump Items match the search criteria, the privileged web access console shows an error message to the user.

All of the search criteria for the `start_jump_item_session` command are supported with `type=web_console`, including:

- `jump.method`
- `search_string`
- `client.hostname`
- `client.comments`
- `client.tag`
- `client.public_ip`
- `client.private_ip`
- `session.custom.<attribute code name>`

Return to an Active Session in the Privileged Web Access Console

If you have multiple access sessions in progress, you have the ability to return to any of these sessions at any time. To return to an endpoint already accessed in another session, click on the session at the top of the screen.



Search for Endpoints

While using the privileged web access console, you can search for specific endpoints while in an access session. Within the search results, you can also click on the **Start** button to begin a session with that endpoint.

1. Click on the **Search** icon located in the top left of the screen.
2. In the search bar, type in the name of the endpoint.
3. From the results provided, select the endpoint you wish to start a session with and click on the **Jump** button to begin a session.



Control the Remote Endpoint with Screen Sharing Using Privileged Web

To view and control remote systems, use the screen sharing action while in an access session.

1. From the session window, click on the **Screen Sharing** tab at the top of the screen. Or, you can click on the **Start Screen Sharing** icon to begin accessing the endpoint if screen sharing does not start automatically.
2. Use any of the following actions while in a session to perform different functions.



Screen Sharing Tools

	Stop screen sharing.
	While viewing the remote computer, start or stop control of the remote keyboard and mouse.
	<p>If your permissions allow, you can disable the remote user's screen view and mouse and keyboard input. The end user's view of the privacy screen clearly explains that the BeyondTrust user has disabled the end user's view. The end user can regain control at any time by pressing Ctrl+Alt+Del.</p> <p>Alternatively, disable the end user's mouse and keyboard input while still allowing them to view the screen. When input is restricted, an orange border appears around the end user's monitors, and a message indicates that the BeyondTrust user has mouse and keyboard control. The end user can regain control at any time by pressing Ctrl+Alt+Del.</p> <p>Restricted endpoint interaction is available only when accessing macOS or Windows computers. Restricted customer interaction is available only when supporting Windows computers. In Windows Vista and above, the endpoint client must be elevated. On Windows 8, this feature is limited to disabling the mouse and keyboard.</p>
	Reboot the remote system in either normal or safe mode with networking, or shut down the remote system.
	Send a Ctrl-Alt-Del command to the remote computer.
	<p>Perform a special action on the remote system. Based on remote operating system and configuration, available tasks will vary. Canned scripts available to the user appear in a fly-out menu. With the Run As special action on a Windows® system, you may select credentials from an Endpoint Credential Manager. Use of the Endpoint Credential Manager requires a separate services agreement with BeyondTrust. Once a services agreement is in place, you may download the required middleware from the BeyondTrust Support Portal.</p>
	Toggle the clipboard.

	Toggle the virtual keyboard.
	Take a screenshot. You can save it to a file or to the clipboard.
	Select an alternate remote monitor to display. The primary monitor is designated by a P .
	View the remote screen at actual or scaled size.
	Select the color optimization mode to view the remote screen. If you are going to be primarily sharing video, select Video Optimized ; otherwise select between Black and White (uses less bandwidth), Few Colors , More Colors , or Full Color (uses more bandwidth). Both Video Optimized and Full Color modes allow you to view the actual desktop wallpaper.
	View the remote desktop in full screen mode or return to the interface view. When in full screen mode, special keys are passed through to the remote system. This includes but is not limited to modifier keys, function keys, and the Windows Start key. Note that this does not apply to the Ctrl-Alt-Del command.

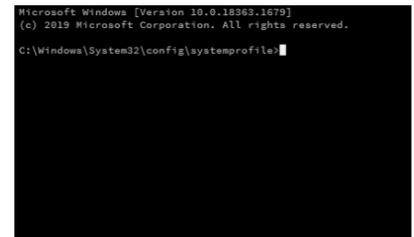
Open the Command Shell on the Remote Endpoint Using the Privileged Web Console

Remote command shell enables a privileged user to open a virtual command line interface to a remote system. The user can then type locally but have the commands executed on the remote system. You can work from multiple shells. Note that scripts available to the user may also be executed on the remote system from the screen sharing interface.

Your administrator can also enable remote shell recording so that a video of each shell can be later viewed from the session report. If shell recording is enabled, a transcript of the command shell will also be available.

 **Note:** Depending on session policy and type of jump, **Command Shell** may not be available.

1. To access the **Command Shell** while in an access session, click on the **Command Shell** tab at the top of the screen.
2. If you are not automatically directed to the command shell, click the **Start the Command Shell** button.
3. The command options and prompt appears.



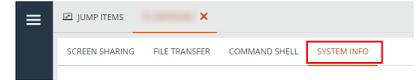
Command Shell Tools

-  Stop command prompt access when it is no longer needed.
-  Open a new shell to run multiple instances of command prompt, or close individual shells without relinquishing command prompt access. Shells are tabulated at the bottom of the screen.

View System Information on the Remote Endpoint

Privileged users can view a complete snapshot of the remote device's or computer's system information to reduce the time needed to diagnose and resolve the issue. The system information available varies depending on the remote operating system and configuration.

1. From the session window, click on the **System Info** tab at the top of the screen. You can click the **Start System Info** button if system information doesn't open automatically.
2. Use any of the following actions while in a session to perform different functions.



System Information Tools

	Refresh system info.
	Copy to clipboard.
	Save to file.

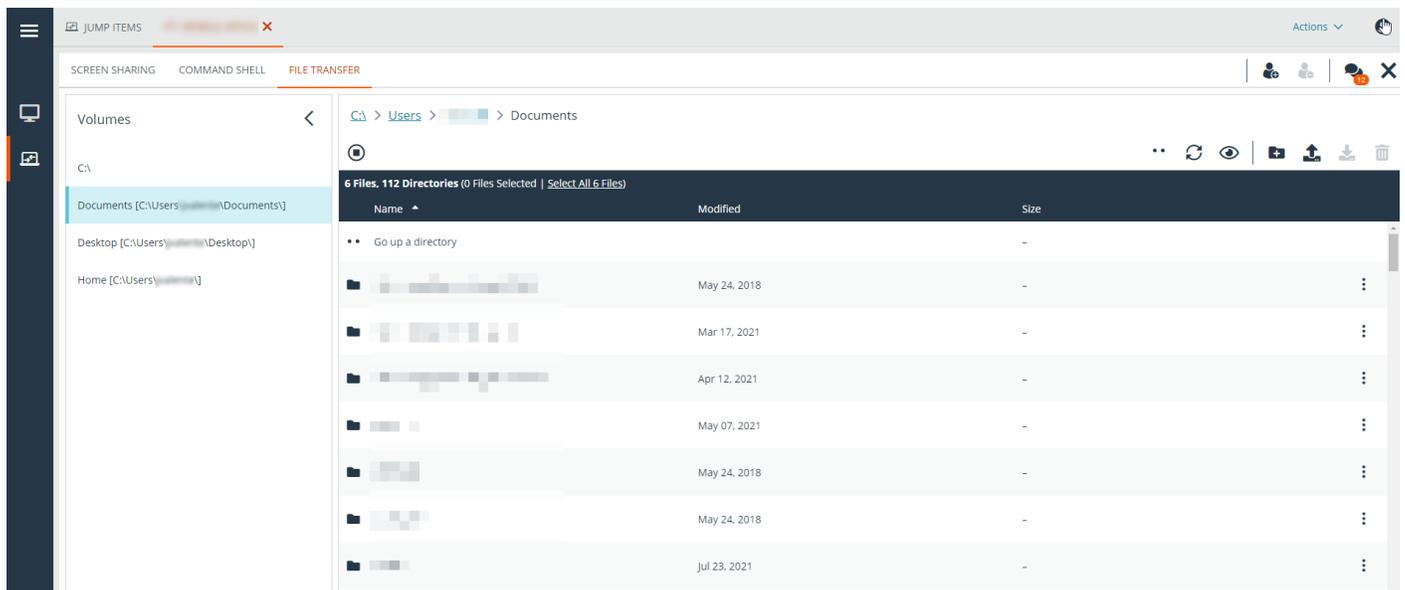
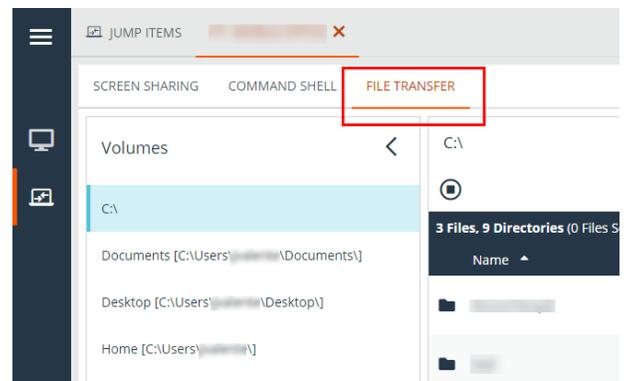
Use the Privileged Web Console to Transfer Files to and from Remote Systems

During a session, privileged users can transfer, delete, or rename files and even entire directories both to and from the remote computer, the remote device, and the device's SD card. You do not have to have full control of the remote computer in order to transfer files.

Depending upon the permissions your administrator has set for your account, you may be only allowed to upload files to the remote system or to download files to your local computer. File system access may also be restricted to certain paths on the remote or local system, thereby restricting uploads and downloads to specific directories. Transfer files by using the upload and download buttons. Review transfer and deletion progress by clicking the plus sign at the bottom of the screen. Download, rename, or delete files by clicking on the **More Options** icon.

To start transferring files to a system, click on the **File Transfer** tab at the top of the screen.

Select a place to start browsing from the **Volumes** column. The breadcrumbs at the top show your current location. Double click on a folder to open it.



File Transfer Tools

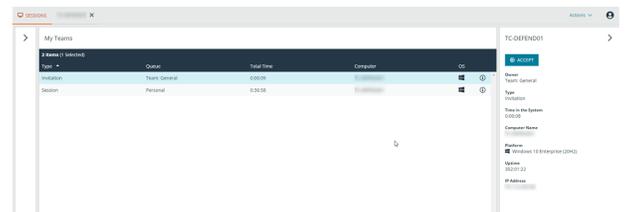
	Stop access to the remote device's file system.
	Go up a directory in the selected file system.
	Refresh your view of the selected file system.
	Show hidden files.
	Create a new directory.
	Upload a file to a directory.
	Download selected files from a directory.
	Delete selected files from a directory.
	Download, rename, or delete a directory or file.
 Note: When deleting a file or folder, it is permanently deleted. It is not sent to the recycle bin.	

Share a Session with Team Members or External Users Using the Privileged Web Access Console

Invite Team Members

Within a session, you can request for a team member to participate in an access session. To share a session, follow the steps outlined below.

1. Click the **Invite other users into this session** icon.
2. Select the team that the user is a member of from the menu.
3. From the team listing, choose the user with whom you would like to share the session.
4. The user being invited will see a notification appear in the lower left corner of the screen indicating they have a new session invitation.
5. Clicking **VIEW** on the notification banner displays information regarding the session. The user can then click **ACCEPT** to enter the session.



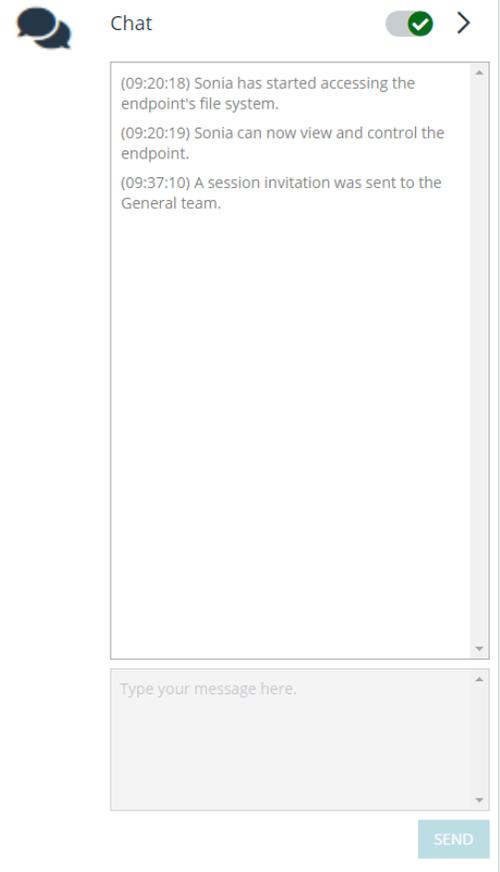
6. Once the user has entered the session, you can chat with them by clicking on the **Chat** icon at the top of the screen.

You can send multiple invitations if you want more members from the team to join your session. Users are listed here only if they are logged into the access console or if they have extended availability enabled.

If you are permitted to share sessions with users who are not members of your teams, additional teams are displayed, provided that they contain at least one member logged into the access console or if they have extended availability enabled.

Only the session owner can send invitations. Invitations do not time out as long as you remain the session owner. Multiple active invitations cannot exist for the same user to join the same session. The invitation will disappear if:

- The inviting user cancels the invitation.
- The inviting user leaves the session.
- The session ends.
- The invited user accepts the invitation.



Invite External Users

You can invite an external user or vendor to participate in an access session. To share a session, follow the steps outlined below:

1. Click the **Invite other users into this session** icon.
2. Select **Invite External User...**

SHARE SESSION

Invite External User...

- ▼ 👤 Support Teams
 - > 👤 Cancel Invitation
 - > 👤 Team: General

CLOSE

INVITE

1. Select a policy, if applicable, and enter a short description for the type of invitation.
2. In the **Invitation Parameters** area, enter the name of the person being invited, plus some comments to go along with the invitation.
3. Click **Create Invitation**.

INVITE EXTERNAL USER

● *Required field*

Select Policy

WorkShare ▼

Description

Session sharing

Invitation Parameters

User's Name ●

Bob

Comments ●

I need help with the new installation.

CANCEL

CREATE INVITATION

You can now invite an external user by either clicking on the **Copy to Clipboard** icon and providing the user with the link to the session URL, or by sending an email invitation.

ACCESS INVITATION GENERATED

You may invite a user to your session by sending them directly to the following URL, or by emailing an invitation.

URL

https://tech [REDACTED] .com 

CLOSE

SEND LOCAL EMAIL

Remove a Member from a Privileged Web Access Console Session

When needed, you can remove another user from a shared access session. To remove a user, click on the **Remove Member** icon.

From the menu, choose the participant you wish to remove. Click **Remove Member**.



Note: *You must be the owner of the session to remove another member.*

Close the Privileged Web Access Console Session

1. To exit an access session, click on the **X** icon in the top right corner of the screen. If you are the session owner, please note that the **End Session** action will close the session page in your access console and will remove any additional members who may be sharing the session.
2. Next, you will receive a prompt asking if you would like to end the session.
3. If you click **OK**, the session will end, and you will be directed back to the **All Jump Items** list.

**END**

Disconnect the endpoint, remove any users from the session, and close this window.

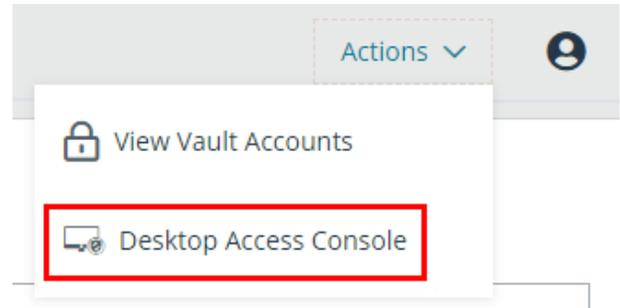
END SESSION

CANCEL

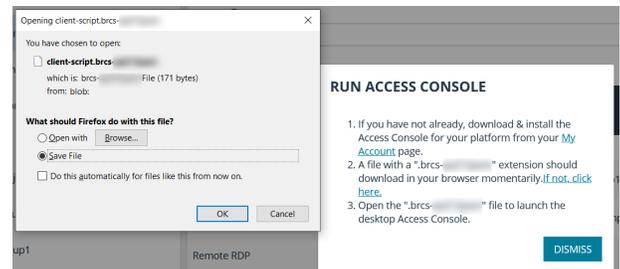
Download the Native Desktop from the Privileged Web Access Console

While working in the privileged web access console, you can choose at any time to download the native desktop access console to your computer.

1. To download the native desktop access console from the privileged web access console, select **Desktop Access Console** located under the **Active** menu in the top right corner of the screen.



2. When the installer appears, follow the instructions to install the software.



Note: On a Linux system, you must save the file to your computer and then open it from its download location. Do not use the **Open** link that appears after downloading a file from some browsers.